Exponential Sums, Cyclic Codes and Sequences: the Odd Characteristic Kasami Case

February 26, 2009

Jinquan Luo Yuansheng Tang and Hongyu Wang

[0]The authors are with the School of Mathematics, Yangzhou University, Jiangsu Province, 225009, China

J.Luo is also with the Division of Mathematics, School of Physics and Mathematical Sciences, Nanyang Technological University, Singapore.

E-mail addresses: jqluo@ntu.edu.sg, ystang@yzu.edu.cn, hywang@yzu.edu.cn.

Abstract

Let $q = p^n$ with $n = 2m$ and p be an odd prime. Let $0 \leq k \leq n-1$ and $k \neq m$. In this paper we determine the value distribution of following exponential(character) sums

$$\sum_{x \in \mathbb{F}_q} \zeta_p^{\mathrm{Tr}_1^m(\alpha x^{p^m+1}) + \mathrm{Tr}_1^n(\beta x^{p^k+1})} \quad (\alpha \in \mathbb{F}_{p^m}, \beta \in \mathbb{F}_q)$$

and

$$\sum_{x \in \mathbb{F}_q} \zeta_p^{\mathrm{Tr}_1^m(\alpha x^{p^m+1}) + \mathrm{Tr}_1^n(\beta x^{p^k+1} + \gamma x)} \quad (\alpha \in \mathbb{F}_{p^m}, \beta, \gamma \in \mathbb{F}_q)$$

where $\mathrm{Tr}_1^n : \mathbb{F}_q \to \mathbb{F}_p$ and $\mathrm{Tr}_1^m : \mathbb{F}_{p^m} \to \mathbb{F}_p$ are the canonical trace mappings and $\zeta_p = e^{\frac{2\pi i}{p}}$ is a primitive p-th root of unity. As applications:

(1). We determine the weight distribution of the cyclic codes $\mathcal{C}_1$ and $\mathcal{C}_2$ over $\mathbb{F}_{p^t}$ with parity-check polynomials $h_2(x)h_3(x)$ and $h_1(x)h_2(x)h_3(x)$ respectively where t is a divisor of $d = \gcd(m, k)$, and $h_1(x)$, $h_2(x)$ and $h_3(x)$ are the minimal polynomials of π^{-1}, $\pi^{-(p^k+1)}$ and $\pi^{-(p^m+1)}$ over $\mathbb{F}_{p^t}$ respectively for a primitive element π of $\mathbb{F}_q$.

(2). We determine the correlation distribution among a family of m-sequences.

This paper extends the results in [30].

Index terms: Exponential sum, Cyclic code, Sequence, Weight distribution, Correlation distribution

1 Introduction

Let C be an $[l,k,d]_{p^t}$ cyclic code and A_i be the number of codewords in $\mathcal{C}$ with Hamming weight i. The weight distribution $\{A_i\}_{i=0}^{l}$ is an important research object in coding theory. If $\mathcal{C}$ is irreducible, which means that the parity-check polynomial of $\mathcal{C}$ is irreducible in $\mathbb{F}_{p^t}[x]$, the weight of each codeword can be expressed by certain conbination of Gaussian sums so that the weight distribution of $\mathcal{C}$ can be determined if the corresponding Gaussian sums can be calculated explicitly (see Fitzgerald and Yucas [5], McEliece [14], McEliece and Rumsey [16], van der Vlugt [24], Wolfmann [26] and the references therein). As for the relationship between the weight distribution of cyclic codes and the rational points of certain curves, see Schoof [22].

For a general cyclic code, the Hamming weight of each codeword can be expressed by certain combination of more general exponential(character) sums (see Feng and Luo [3], [4], Luo and Feng [9], [10], van der Vlugt [25], Yuan, Carlet and Ding [28]). More exactly speaking, let $q = p^n$ with $t \mid n$, $\mathcal{C}$ be the cyclic code over $\mathbb{F}_{p^t}$ with length $l = q-1$ and parity-check polynomial

$$h(x) = h_1(x) \cdots h_u(x) \quad (u \geq 2)$$

where $h_i(x)$ $(1 \leq i \leq e)$ are distinct irreducible polynomials in $\mathbb{F}_{p^t}[x]$ with degree e_i $(1 \leq i \leq u)$, then $\dim_{\mathbb{F}_{p^t}} \mathcal{C} = \sum\limits_{i=1}^{u} e_i$. Let π be a primitive element of $\mathbb{F}_q$ and π^{-s_i} be a zero of $h_i(x)$, $1 \leq s_i \leq q-2$ $(1 \leq i \leq u)$. Then the codewords in $\mathcal{C}$ can be expressed by

$$c(\alpha_1, \cdots, \alpha_u) = (c_0, c_1, \cdots, c_{l-1}) \quad (\alpha_1, \cdots, \alpha_u \in \mathbb{F}_q)$$

where $c_i = \sum\limits_{\lambda=1}^{u} \mathrm{Tr}_t^n(\alpha_\lambda \pi^{is_\lambda})$ $(0 \leq i \leq n-1)$ and $\mathrm{Tr}_j^h : \mathbb{F}_{p^h} \to \mathbb{F}_{p^j}$ is the trace mapping for positive integers $j \mid h$. Therefore the Hamming weight of the codeword

$c = c(\alpha_1, \cdots, \alpha_u)$ is

$$\begin{aligned}
w_H(c) &= \#\{i \,|0 \le i \le l-1, c_i \ne 0\} \\
&= l - \#\{i \,|0 \le i \le l-1, c_i = 0\} \\
&= l - \frac{1}{p^t} \sum_{i=0}^{l-1} \sum_{a \in \mathbb{F}_{p^t}} \zeta_p^{\mathrm{Tr}_1^t\left(a \cdot \mathrm{Tr}_t^n\left(\sum\limits_{\lambda=1}^{u} \alpha_\lambda \pi^{i s_\lambda}\right)\right)} \\
&= l - \frac{l}{p^t} - \frac{1}{p^t} \sum_{a \in \mathbb{F}_{p^t}^*} \sum_{x \in \mathbb{F}_q^*} \zeta_p^{\mathrm{Tr}_1^n(af(x))} \\
&= l - \frac{l}{p^t} + \frac{p^t - 1}{p^t} - \frac{1}{p^t} \sum_{a \in \mathbb{F}_{p^t}^*} S(a\alpha_1, \cdots, a\alpha_u) \\
&= p^{n-t}(p^t - 1) - \frac{1}{p^t} \sum_{a \in \mathbb{F}_{p^t}^*} S(a\alpha_1, \cdots, a\alpha_u) \qquad (1)
\end{aligned}$$

where $f(x) = \alpha_1 x^{s_1} + \alpha_2 x^{s_2} + \cdots + \alpha_u x^{s_u} \in \mathbb{F}_q[x]$, $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$, $\mathbb{F}_{p^t}^* = \mathbb{F}_{p^t} \backslash \{0\}$, and

$$S(\alpha_1, \cdots, \alpha_u) = \sum_{x \in \mathbb{F}_q} \zeta_p^{\mathrm{Tr}_1^n(\alpha_1 x^{s_1} + \cdots + \alpha_u x^{s_u})}.$$

In this way, the weight distribution of cyclic code $\mathcal{C}$ can be derived from the explicit evaluating of the exponential sums

$$S(\alpha_1, \cdots, \alpha_u) \quad (\alpha_1, \cdots, \alpha_u \in \mathbb{F}_q).$$

Let $n = 2m, 0 \le k \le n-1, k \ne m$, p be an odd prime, $d = \gcd(k, m)$ and $q_0 = p^d$. Define $s = n/d$. Then we have $q = q_0^s$. Assume t is a divisor of d and $n_0 = n/t$. Let $h_1(x)$, $h_2(x)$ and $h_3(x)$ be the minimal polynomials of $\pi^{-1}, \pi^{-(p^k+1)}$ and $\pi^{-(p^m+1)}$ over $\mathbb{F}_{p^t}$ respectively. Then

$$\deg h_i(x) = n_0 \text{ for } i = 1, 2 \text{ and } \deg h_3(x) = n_0/2 \qquad (2)$$

Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be the cyclic codes over $\mathbb{F}_{p^t}$ with length $l = q-1$ and parity-check polynomials $h_2(x)h_3(x)$ and $h_1(x)h_2(x)h_3(x)$ respectively. From (2), we know that the dimensions of $\mathcal{C}_1$ and $\mathcal{C}_2$ over $\mathbb{F}_{p^t}$ are $3n_0/2$ and $5n_0/2$ respectively.

For $\alpha \in \mathbb{F}_{p^m}, (\beta, \gamma) \in \mathbb{F}_q^2$, define the exponential sums

$$T(\alpha, \beta) = \sum_{x \in \mathbb{F}_q} \zeta_p^{\mathrm{Tr}_1^m(\alpha x^{p^m+1}) + \mathrm{Tr}_1^n(\beta x^{p^k+1})} \qquad (3)$$

and

$$S(\alpha,\beta,\gamma)=\sum_{x\in\mathbb{F}_q}\zeta_p^{\mathrm{Tr}_1^m(\alpha x^{p^m+1})+\mathrm{Tr}_1^n(\beta x^{p^k+1}+\gamma x)}. \tag{4}$$

Then the weight distribution of $\mathcal{C}_1$ and $\mathcal{C}_2$ can be completely determined if $T(\alpha,\beta)$ and $S(\alpha,\beta,\gamma)$ are explicitly evaluated.

Another application of $S(\alpha,\beta,\gamma)$ is to calculate the correlation distribution of corresponding sequences. Let $\mathcal{F}$ be a collection of p-ary m-sequences of period $q-1$ defined by

$$\mathcal{F}=\left\{\{a_i(t)\}_{i=0}^{q-2}\,|\,0\le i\le L-1\right\}$$

The *correlation function* of a_i and a_j for a shift τ is defined by

$$M_{i,j}(\tau)=\sum_{\lambda=0}^{q-2}\zeta_p^{a_i(\lambda)-a_j(\lambda+\tau)}\qquad\qquad (0\le\tau\le q-2).$$

In this paper, we will study the collection of sequences

$$\mathcal{F}=\left\{a_{\alpha,\beta}=\left\{a_{\alpha,\beta}(\pi^\lambda)\right\}_{\lambda=0}^{q-2}\,|\,\alpha\in\mathbb{F}_{p^m},\beta\in\mathbb{F}_q\right\} \tag{5}$$

where $a_{\alpha,\beta}(\pi^\lambda)=\mathrm{Tr}_1^m(\alpha\pi^{\lambda(p^m+1)})+\mathrm{Tr}_1^n(\beta\pi^{\lambda(p^k+1)}+\pi^\lambda)$.

Then the correlation function between a_{α_1,β_1} and a_{α_2,β_2} by a shift τ $(0\le\tau\le q-2)$ is

$$\begin{aligned}M_{(\alpha_1,\beta_1),(\alpha_2,\beta_2)}(\tau)&=\sum_{\lambda=0}^{q-2}\zeta_p^{a_{\alpha_1,\beta_1}(\lambda)-a_{\alpha_2,\beta_2}(\lambda+\tau)}\\&=\sum_{\lambda=0}^{q-2}\zeta_p^{\mathrm{Tr}_1^m(\alpha_1\pi^{\lambda(p^m+1)})+\mathrm{Tr}_1^n(\beta_1\pi^{\lambda(p^k+1)}+\pi^\lambda)-\mathrm{Tr}_1^m(\alpha_2\pi^{(\lambda+\tau)(p^m+1)})-\mathrm{Tr}_1^n(\beta\pi^{(\lambda+\tau)(p^k+1)}+\pi^{\lambda+\tau})}\\&=S(\alpha',\beta',\gamma')-1\end{aligned} \tag{6}$$

where

$$\alpha'=\alpha_1-\alpha_2\pi^{\tau(p^m+1)},\quad \beta'=\beta_1-\beta_2\pi^{\tau(p^k+1)},\quad \gamma'=1-\pi^\tau. \tag{7}$$

Pairs of p-ary m-sequences with few-valued cross correlations have been extensively studied for several decades, see Gold [6], Helleseth and Kumar [7], Helleseth, Lahtonen and Rosendahl [8], Kasami [12], Rosendahl [20], [21] and Trachtenberg [23].

Several special cases of exponential sums (4) and related cyclic code $\mathcal{C}_2$ have been investigated, for instance

- The binary code $\mathcal{C}_2$ with $k = m \pm 1$ is nothing but the classical Kasami code, see Kasami [12].
- As for the binary code $\mathcal{C}_2$ with $k = 1$, its minimal distance is obtained by Lahtonen [15], Moreno and Kumar [17]. Its weight distribution is determined eventually in van der Vlugt [25].
- For several other cases, the binary code $\mathcal{C}_2$ and the related family of generalized Kasami sequences have been studied, see Zeng, Liu and Hu [29].
- In the case p odd prime and $\gcd(m, k) = \gcd(m + k, 2k) = d$ being odd, the weight distribution of $\mathcal{C}_2$ and correlation distribution of corresponding sequences have been fully determined, see Zeng, Li and Hu [30].

This paper is presented as follows. In Section 2 we introduce some preliminaries. In Section 3 we will study the value distribution of $T(\alpha, \beta)$ (that is, which value $T(\alpha, \beta)$ takes on and which frequency of each value for $\alpha \in \mathbb{F}_{p^m}, \beta \in \mathbb{F}_q$) and the weight distribution of $\mathcal{C}_1$. In Section 3 we will determine the value distribution of $S(\alpha, \beta, \gamma)$, the correlation distribution among the sequences in $\mathcal{F}$, and then the weight distribution of $\mathcal{C}_2$. Most lengthy details are presented in several appendixes. The main tools are quadratic form theory over finite fields of odd characteristic, some moment identities on $T(\alpha, \beta)$ and a class of Artin-Schreier curves on finite fields. We will focus our study on the odd prime characteristic case and the binary case will be investigated in a following paper.

2 Preliminaries

We follow the notations in Section 1. The first machinery to determine the values of exponential sums $T(\alpha, \beta)$ and $S(\alpha, \beta, \gamma)$ defined in (3) and (4) is quadratic form theory over $\mathbb{F}_{q_0}$.

Let H be an $s \times s$ symmetric matrix over $\mathbb{F}_{q_0}$ and $r = \operatorname{rank} H$. Then there exists $M \in \mathrm{GL}_s(\mathbb{F}_{q_0})$ such that $H' = MHM^T$ is diagonal and $H' = diag(a_1, \cdots, a_r, 0, \cdots, 0)$ where $a_i \in \mathbb{F}_{q_0}^*$ $(1 \leq i \leq r)$. Let $\Delta = a_1 \cdots a_r$ (we assume $\Delta = 1$ when $r = 0$) and η_0 be the quadratic (multiplicative) character of $\mathbb{F}_{q_0}$. Then $\eta_0(\Delta)$ is an invariant of H under the conjugate action of $M \in \mathrm{GL}_s(\mathbb{F}_{q_0})$.

For the quadratic form

$$F : \mathbb{F}_{q_0}^s \to \mathbb{F}_{q_0}, \quad F(x) = XHX^T \quad (X = (x_1, \cdots, x_s) \in \mathbb{F}_{q_0}^s), \tag{8}$$

we have the following result(see [9], Lemma 1).

***Lemma* 1.** *(i). For the quadratic form $F = XHX^T$ defined in (8), we have*

$$\sum_{X\in\mathbb{F}_{q_0}^s} \zeta_p^{\mathrm{Tr}_1^d(F(X))} = \begin{cases} \eta_0(\Delta)q_0^{s-r/2} & \text{if } q_0 \equiv 1 \pmod 4, \\ i^r\eta_0(\Delta){q_0}^{s-r/2} & \text{if } q_0 \equiv 3 \pmod 4. \end{cases}$$

(ii). For $A = (a_1, \cdots, a_s) \in \mathbb{F}_{q_0}^s$, if $2YH + A = 0$ has solution $Y = B \in \mathbb{F}_{q_0}^s$, then $\sum_{X\in\mathbb{F}_{q_0}^s} \zeta_p^{\mathrm{Tr}_1^d(F(X)+AX^T)} = \zeta_p^c \sum_{X\in\mathbb{F}_{q_0}^s} \zeta_p^{\mathrm{Tr}_1^d(F(X))}$ where $c = -\mathrm{Tr}_1^d\left(BHB^T\right) = \frac{1}{2}\mathrm{Tr}_1^d\left(AB^T\right) \in \mathbb{F}_p$.

Otherwise $\sum_{X\in\mathbb{F}_p^m} \zeta_p^{\mathrm{Tr}_1^d(F(X)+AX^T)} = 0$.

In this correspondence we always assume $d = \gcd(m, k)$. Recall that $s = n/d$ is even. Therefore the field $\mathbb{F}_q$ is a vector space over $\mathbb{F}_{q_0}$ with dimension s. We fix a basis $v_1, \cdots, v_s$ of $\mathbb{F}_q$ over $\mathbb{F}_{q_0}$. Then each $x \in \mathbb{F}_q$ can be uniquely expressed as

$$x = x_1v_1 + \cdots + x_sv_s \quad (x_i \in \mathbb{F}_{q_0}).$$

Thus we have the following $\mathbb{F}_{q_0}$-linear isomorphism:

$$\mathbb{F}_q \xrightarrow{\sim} \mathbb{F}_{q_0}^s, \quad x = x_1v_1 + \cdots + x_sv_s \mapsto X = (x_1, \cdots, x_s).$$

With this isomorphism, a function $f : \mathbb{F}_q \to \mathbb{F}_{q_0}$ induces a function $F : \mathbb{F}_{q_0}^s \to \mathbb{F}_{q_0}$ where for $X = (x_1, \cdots, x_s) \in \mathbb{F}_{q_0}^s$, $F(X) = f(x)$ with $x = x_1v_1 + \cdots + x_sv_s$. In this way, function $f(x) = \mathrm{Tr}_d^n(\gamma x)$ for $\gamma \in \mathbb{F}_q$ induces a linear form

$$F(X) = \mathrm{Tr}_d^n(\gamma x) = \sum_{i=1}^s \mathrm{Tr}_d^n(\gamma v_i)x_i = A_\gamma X^T \tag{9}$$

where $A_\gamma = (\mathrm{Tr}_d^n(\gamma v_1), \cdots, \mathrm{Tr}_d^n(\gamma v_s))$, and $f_{\alpha,\beta}(x) = \mathrm{Tr}_d^m(\alpha x^{p^m+1}) + \mathrm{Tr}_d^n(\beta x^{p^k+1})$ for $\alpha \in \mathbb{F}_{p^m}$, $\beta \in \mathbb{F}_q$ induces a quadratic form

$$\begin{aligned} F_{\alpha,\beta}(X) &= \mathrm{Tr}_d^m(\alpha x^{p^m+1}) + \mathrm{Tr}_d^n(\beta x^{p^k+1}) \\ &= \mathrm{Tr}_d^m\left(\alpha\left(\sum_{i=1}^s x_iv_i^{p^m}\right)\left(\sum_{i=1}^s x_iv_i\right)\right) + \mathrm{Tr}_d^n\left(\left(\beta\sum_{i=1}^s x_iv_i^{p^k}\right)\left(\sum_{i=1}^s x_iv_i\right)\right) \\ &= \sum_{i,j=1}^s \left(\frac{1}{2}\mathrm{Tr}_d^m\left(\alpha v_i^{p^m}v_j + \alpha v_iv_j^{p^m}\right) + \mathrm{Tr}_d^n\left(\beta v_i^{p^k}v_j\right)\right)x_ix_j = XH_{\alpha,\beta}X^T \end{aligned} \tag{10}$$

where

$$H_{\alpha,\beta}=(h_{ij}) \text{ and } h_{ij}=\frac{1}{2}\operatorname{Tr}_d^m\left(\alpha v_i^{p^m}v_j+\alpha v_i v_j^{p^m}\right)+\frac{1}{2}\operatorname{Tr}_d^n\left(\beta v_i^{p^k}v_j+\beta v_i v_j^{p^k}\right) \text{ for } 1\leq i,j\leq s.$$

From Lemma 1, in order to determine the values of

$$T(\alpha,\beta)=\sum_{x\in\mathbb{F}_q}\zeta_p^{\operatorname{Tr}_1^m(\alpha x^{p^m+1})+\operatorname{Tr}_1^n(\beta x^{p^k+1})}=\sum_{X\in\mathbb{F}_{q_0}^s}\zeta_p^{\operatorname{Tr}_1^d\left(XH_{\alpha,\beta}X^T\right)}$$

and

$$S(\alpha,\beta,\gamma)=\sum_{x\in\mathbb{F}_q}\zeta_p^{\operatorname{Tr}_1^m(\alpha x^{p^m+1})+\operatorname{Tr}_1^n(\beta x^{p^k+1}+\gamma x)}=\sum_{X\in\mathbb{F}_p^m}\zeta_p^{\operatorname{Tr}_1^d\left(XH_{\alpha,\beta}X^T+A_\gamma X^T\right)}\quad(\alpha\in\mathbb{F}_{p^m},\beta,\gamma\in\mathbb{F}_q),$$

we need to determine the rank of $H_{\alpha,\beta}$ over $\mathbb{F}_{q_0}$ and the solvability of $\mathbb{F}_{q_0}$-linear equation $2XH_{\alpha,\beta}+A_\gamma=0$.

Define $d'=\gcd(m+k,2k)$. Then an easy observation shows

$$d'=\begin{cases}2d, & \text{if } m/d \text{ and } k/d \text{ are both odd;}\\ d, & \text{otherwise.}\end{cases}\tag{11}$$

The main part of the subsequent result has been proven in [30] and we repeat part of the proof for self-containing.

Lemma 2. *For $(\alpha,\beta)\in\mathbb{F}_{p^m}\times\mathbb{F}_q\backslash\{(0,0)\}$, let $r_{\alpha,\beta}$ be the rank of $H_{\alpha,\beta}$. Then we have*

(i). if $d'=d$, then the possible values of $r_{\alpha,\beta}$ are s, $s-1$, $s-2$.

(ii). if $d'=2d$, then the possible values of $r_{\alpha,\beta}$ are s, $s-2$, $s-4$.

Moreover, let n_i be the number of (α,β) with $r_{\alpha,\beta}=s-i$. In the case $d'=d$, we have $n_1=p^{m-d}(p^n-1)$.

Proof. see **Appendix A.** □

In order to determine the value distribution of $T(\alpha,\beta)$ for $\alpha\in\mathbb{F}_{p^m},\beta\in\mathbb{F}_q$, we need the following result on moments of $T(\alpha,\beta)$.

Lemma 3. *For the exponential sum $T(\alpha,\beta)$,*

(i). $$\sum_{\alpha\in\mathbb{F}_{p^m},\beta\in\mathbb{F}_q} T(\alpha,\beta)=p^{3m};$$

(ii). $$\sum_{\alpha\in\mathbb{F}_{p^m},\beta\in\mathbb{F}_q} T(\alpha,\beta)^2=\begin{cases} p^{3m} & \text{if } d'=d \text{ and } p^d\equiv 3 \pmod 4,\\ (2p^n-1)\cdot p^{3m} & \text{if } d'=d \text{ and } p^d\equiv 1 \pmod 4,\\ (p^{n+d}+p^n-p^d)\cdot p^{3m} & \text{if } d'=2d;\end{cases}$$

(iii). *if $d'=d$, then*

$$\sum_{\alpha\in\mathbb{F}_{p^m},\beta\in\mathbb{F}_q} T(\alpha,\beta)^3=(p^{n+d}+p^n-p^d)\cdot p^{3m}.$$

Proof. see **Appendix A.** □

In the case $d'=2d$, we could determine the explicit values of $T(\alpha,\beta)$. To this end we will study a class of Artin-Schreier curves. A similar technique has been applied in Coulter [2], Theorem 6.1.

Lemma 4. *Suppose $(\alpha,\beta)\in(\mathbb{F}_{p^m}\times\mathbb{F}_q)\setminus\{0,0\}$ and $d'=2d$. Let N be the number of $\mathbb{F}_q$-rational (affine) points on the curve*

$$\frac{1}{2}\alpha x^{p^m+1}+\beta x^{p^k+1}=y^{p^d}-y. \tag{12}$$

Then

$$N=q+(p^d-1)\cdot T(\alpha,\beta).$$

Proof. see **Appendix A.** □

Now we give an explicit evaluation of $T(\alpha,\beta)$ in the case $d'=2d$.

Lemma 5. *Assumptions as in Lemma 4, then*

$$T(\alpha,\beta)=\begin{cases} -p^m, & \text{if } r_{\alpha,\beta}=s\\ p^{m+d}, & \text{if } r_{\alpha,\beta}=s-2\\ -p^{m+2d}, & \text{if } r_{\alpha,\beta}=s-4\end{cases}$$

Proof. Consider the $\mathbb{F}_q$-rational (affine) points on the Artin-Schreier curve in Lemma 4. It is easy to verify that $(0,y)$ with $y\in\mathbb{F}_{p^d}$ are exactly the points on the curve with $x=0$. If (x,y) with $x\neq 0$ is a point on this curve, then so are

$(tx, t^{p^d+1}y)$ with $t^{p^{2d}-1} = 1$ (note that $p^m + 1 \equiv p^k + 1 \equiv p^d + 1 \pmod{p^{2d} - 1}$ since m/d and k/d are both odd by (11)). In total, we have

$$q + (p^d - 1)T(\alpha, \beta) = N \equiv p^d \pmod{p^{2d} - 1}$$

which yields

$$T(\alpha, \beta) \equiv 1 \pmod{p^d + 1}.$$

We only consider the case $r_{\alpha,\beta} = s$. The other cases are similar. In this case $T(\alpha, \beta) = \pm p^m$. Assume $T(\alpha, \beta) = p^m$. Then $p^d + 1 \mid p^m - 1$ which contradicts to m/d is odd. Therefore $T(\alpha, \beta) = -p^m$. □

Remark. (i). Our treatment improve the technique in [2]. Otherwise the case $(p, d) = (3, 1)$ will be excluded.

(ii). Applying Lemma 5 to Lemma 4, we could determine the number of rational points on the curve (12).

3 Exponential Sums $T(\alpha, \beta)$ and Cyclic Code $\mathcal{C}_1$

Recall $q_0^* = (-1)^{\frac{q_0-1}{2}} q_0$. In this section we prove the following results.

Theorem 1. *The value distribution of the multi-set $\{T(\alpha, \beta) \,|\, \alpha, \beta \in \mathbb{F}_q\}$ is shown as following.*

(i). For the case $d' = d$,

values	*multiplicity*
p^m	$p^d(p^m - 1)(p^m + 1)^2 / \left(2(p^d + 1)\right)$
$-p^m$	$p^d(p^m - 1)(p^n - 2p^{n-d} + 1) / \left(2(p^d - 1)\right)$
$\sqrt{q_0{}^*}{q_0}^{\frac{s}{2}}, -\sqrt{q_0{}^*}{q_0}^{\frac{s}{2}}$	$\frac{1}{2}p^{m-d}(p^n - 1)$
$-p^{m+d}$	$(p^{m-d} - 1)(p^n - 1) / \left(p^{2d} - 1\right)$
p^n	1

(ii). For the case $d' = 2d$,

values	multiplicity
$-p^m$	$p^{3d}(p^m-1)(p^n-p^{n-2d}-p^{n-3d}+p^m-p^{m-d}+1)\big/\big((p^d+1)(p^{2d}-1)\big)$
p^{m+d}	$p^d(p^n-1)(p^m+p^{m-d}+p^{m-2d}+1)/(p^d+1)^2$
$-p^{m+2d}$	$(p^{m-d}-1)(p^n-1)\big/\big((p^d+1)(p^{2d}-1)\big)$
p^n	1

Proof. see **Appendix B.** $\square$

Recall that t is a divisor of d and $\mathcal{C}_1$ is the cyclic code over $\mathbb{F}_{p^t}$ with parity-check polynomial $h_2(x)h_3(x)$ where $h_2(x)$ and $h_3(x)$ are the minimal polynomials of $\pi^{-(p^k+1)}$ and $\pi^{-(p^m+1)}$, respectively.

Theorem 2. *For $k \neq m$, the weight distribution $\{A_0, A_1, \cdots, A_l\}$ of the cyclic code $\mathcal{C}_1$ over $\mathbb{F}_{p^t}$ $(p \geq 3)$ with length $l = q-1$ and $\dim_{\mathbb{F}_{p^t}}\mathcal{C}_1 = 3n_0/2$ is shown as following.*

(i). For the case $d' = d$ and d/t is odd,

i	A_i
$(p^t-1)(p^{n-t}-p^{m-t})$	$p^d(p^m-1)(p^m+1)^2\big/\big(2(p^d+1)\big)$
$(p^t-1)p^{n-t}$	$p^{m-d}(p^n-1)$
$(p^t-1)(p^{n-t}+p^{m-t})$	$p^d(p^m-1)(p^n-2p^{n-d}+1)\big/\big(2(p^d-1)\big)$
$(p^t-1)(p^{n-t}+p^{m+d-t})$	$(p^{m-d}-1)(p^n-1)\big/\big(p^{2d}-1\big)$
0	1

(ii). For the case $d' = d$ and d/t is even,

i	A_i
$(p^t-1)(p^{n-t}-p^{m+\frac{d}{2}-t})$	$\frac{1}{2}p^{m-d}(p^n-1)$
$(p^t-1)(p^{n-t}-p^{m-t})$	$p^d(p^m-1)(p^m+1)^2\big/\big(2(p^d+1)\big)$
$(p^t-1)(p^{n-t}+p^{m-t})$	$p^d(p^m-1)(p^n-2p^{n-d}+1)\big/\big(2(p^d-1)\big)$
$(p^t-1)(p^{n-t}+p^{m+\frac{d}{2}-t})$	$\frac{1}{2}p^{m-d}(p^n-1)$
$(p^t-1)(p^{n-t}+p^{m+d-t})$	$(p^{m-d}-1)(p^n-1)\big/\big(p^{2d}-1\big)$
0	1

(iii). For the case $d' = 2d$,

i	A_i
$(p^t-1)(p^{n-t}-p^{m+d-t})$	$p^d(p^n-1)(p^m+p^{m-d}+p^{m-2d}+1)/(p^d+1)^2$
$(p^t-1)(p^{n-t}+p^{m-t})$	$p^{3d}(p^m-1)(p^n-p^{n-2d}-p^{n-3d}+p^m-p^{m-d}+1)/\big((p^d+1)(p^{2d}-1)\big)$
$(p^t-1)(p^{n-t}+p^{m+2d-t})$	$(p^{m-d}-1)(p^n-1)/\big((p^d+1)(p^{2d}-1)\big)$
0	1

Proof. see **Appendix B.** $\square$

Remark. (1). In the case $d = d'$. Since $\gcd(p^m+1, p^k+1) = 2$, the first $l' = \frac{q-1}{2}$ coordinates of each codeword of $\mathcal{C}_1$ form a cyclic code $\mathcal{C}_1'$ over $\mathbb{F}_{p^t}$ with length l' and dimension $3n_0/2$. Let $(A_0', \cdots, A_{l'}')$ be the weight distribution of $\mathcal{C}_1'$, then $A_i' = A_{2i}$ $(0 \le i \le l')$.

(2). In the case $d' = 2d$. Since $\gcd(p^m+1, p^k+1) = p^d+1$, the first $l' = \frac{q-1}{p^d+1}$ coordinates of each codeword of $\mathcal{C}_1$ form a cyclic code $\mathcal{C}_1'$ over $\mathbb{F}_{p^t}$ with length l' and dimension $3n_0/2$. Let $(A_0', \cdots, A_{l'}')$ be the weight distribution of $\mathcal{C}_1'$, then $A_i' = A_{(p^d+1)i}$ $(0 \le i \le l')$.

(2). If $k = 0$, this result is the same as [9], Theorem 3.

4 Results on Correlation Distribution of Sequences and Cyclic Code $\mathcal{C}_2$

Recall $\phi_{\alpha,\beta}(x)$ in the proof of Lemma 2 and $N_{i,\varepsilon}$ in the proof of Theorem 1. Finally we will determine the value distribution of $S(\alpha, \beta, \gamma)$, the correlation distribution among sequences in $\mathcal{F}$ defined in (5) and the weight distribution of $\mathcal{C}_2$ defined in Section 1. The following result will play an important role.

Lemma 6. *Let t be a divisor of d. For any $a \in \mathbb{F}_{p^t}$ and any $(\alpha, \beta) \in N_{i,\varepsilon}$ with $\varepsilon = \pm 1$ and $0 \le i \le 4$, then the number of elements $\gamma \in \mathbb{F}_q$ satisfying*

(i). $\phi_{\alpha,\beta}(x) + \gamma = 0$ is solvable(choose one solution, say x_0),

(ii). $\mathrm{Tr}_t^m(\alpha x_0^{p^m+1}) + \mathrm{Tr}_t^n(\beta x_0^{p^k+1}) = a$

is

$$\begin{cases} p^{n-id-t} & \text{if } s-i \text{ and } d/t \text{ are both odd, and } a=0,\\ p^{n-id-t}+\varepsilon\eta'(a)p^{\frac{n-id-t}{2}} & \text{if } s-i \text{ and } d/t \text{ are both odd, and } a\neq 0,\\ p^{n-id-t}+\varepsilon(p^t-1)p^{\frac{n-id}{2}-t} & \text{if } s-i \text{ or } d/t \text{ is even, and } a=0,\\ p^{n-id-t}-\varepsilon p^{\frac{n-id}{2}-t} & \text{if } s-i \text{ or } d/t \text{ is even, and } a\neq 0.\end{cases}$$

where η' is the quadratic (multiplicative) character on $\mathbb{F}_{p^t}$.

Proof. see **Appendix C.** $\square$

Let $p^* = (-1)^{\frac{p-1}{2}}p$ and $\left(\frac{\cdot}{p}\right)$ be the Legendre symbol. We are now ready to give the value distribution of $S(\alpha,\beta,\gamma)$.

Theorem 3. *The value distribution of the multi-set $\left\{S(\alpha,\beta,\gamma)\,\middle|\,\alpha\in\mathbb{F}_{p^m},(\beta,\gamma)\in\mathbb{F}_q^2\right\}$ is shown as following.*

(i). If $d'=d$ is odd, then

values	*multiplicity*
p^m	$p^{m+d-1}(p^m+1)(p^m+p-1)(p^n-1)\big/\left(2(p^d+1)\right)$
$-p^m$	$p^{m+d-1}(p^m-1)(p^m-p+1)(p^n-2p^{n-d}+1)\big/\left(2(p^d-1)\right)$
$\zeta_p^j p^m$	$p^{m+d-1}(p^n-1)^2\big/\left(2(p^d+1)\right)$
$-\zeta_p^j p^m$	$p^{m+d-1}(p^n-1)(p^n-2p^{n-d}+1)\big/\left(2(p^d-1)\right)$
$\varepsilon\sqrt{p^*}p^{m+\frac{d-1}{2}}$	$\frac{1}{2}p^{3m-2d-1}(p^n-1)$
$\varepsilon\zeta_p^j\sqrt{p^*}p^{m+\frac{d-1}{2}}$	$\frac{1}{2}p^{n-\frac{3d+1}{2}}\left(p^{m-\frac{d+1}{2}}+\varepsilon\left(\frac{-j}{p}\right)\right)(p^n-1)$
$-p^{m+d}$	$p^{m-d-1}(p^{m-d}-1)(p^n-1)(p^{m-d}-p+1)\big/\left(p^{2d}-1\right)$
$-\zeta_p^j p^{m+d}$	$p^{m-d-1}(p^{n-2d}-1)(p^n-1)\big/\left(p^{2d}-1\right)$
0	$(p^n-1)(p^{3m-d}-p^{3m-2d}+p^{3m-3d}-p^{n-2d}+1)$
p^n	1

where $\varepsilon=\pm1, 1\leq j\leq p-1$.

(ii). If $d'=d$ is even, then

values	multiplicity
p^m	$p^{m+d-1}(p^m+1)(p^m+p-1)(p^n-1)\big/\big(2(p^d+1)\big)$
$-p^m$	$p^{m+d-1}(p^m-1)(p^m-p+1)(p^n-2p^{n-d}+1)\big/\big(2(p^d-1)\big)$
$\zeta_p^j p^m$	$p^{m+d-1}(p^n-1)^2\big/\big(2(p^d+1)\big)$
$-\zeta_p^j p^m$	$p^{m+d-1}(p^n-1)(p^n-2p^{n-d}+1)\big/\big(2(p^d-1)\big)$
$\varepsilon p^{m+\frac{d}{2}}$	$\frac{1}{2}p^{n-\frac{3d}{2}-1}(p^{m-\frac{d}{2}}+\varepsilon(p-1))(p^n-1)$
$\varepsilon\zeta_p^j p^{m+\frac{d}{2}}$	$\frac{1}{2}p^{n-\frac{3d}{2}-1}(p^{m-\frac{d}{2}}-\varepsilon)(p^n-1)$
$-p^{m+d}$	$p^{m-d-1}(p^{m-d}-1)(p^n-1)(p^{m-d}-p+1)\big/\big(p^{2d}-1\big)$
$-\zeta_p^j p^{m+d}$	$p^{m-d-1}(p^{m-d}-1)(p^n-1)(p^{m-d}+1)\big/\big(p^{2d}-1\big)$
0	$(p^n-1)(p^{3m-d}-p^{3m-2d}+p^{3m-3d}-p^{n-2d}+1)$
p^n	1

where $\varepsilon=\pm1, 1\leq j\leq p-1$.

(iii). If $d'=2d$, *then*

values	multiplicity
$-p^m$	$p^{m+3d-1}(p^m-1)(p^m-p+1)(p^n-p^{n-2d}-p^{n-3d}+p^m-p^{m-d}+1)\big/(p^d+1)(p^{2d}-1)$
$-\zeta_p^j p^m$	$p^{m+3d-1}(p^n-1)(p^n-p^{n-2d}-p^{n-3d}+p^m-p^{m-d}+1)\big/(p^d+1)(p^{2d}-1)$
p^{m+d}	$p^{m-1}(p^n-1)(p^{m-d}+p-1)(p^m+p^{m-d}+p^{m-2d}+1)\big/(p^d+1)^2$
$\zeta_p^j p^{m+d}$	$p^{m-1}(p^n-1)(p^{m-d}-1)(p^m+p^{m-d}+p^{m-2d}+1)\big/(p^d+1)^2$
$-p^{m+2d}$	$p^{m-2d-1}(p^{m-d}-1)(p^{m-2d}-p+1)(p^n-1)\big/\big((p^d+1)(p^{2d}-1)\big)$
$-\zeta_p^j p^{m+2d}$	$p^{m-2d-1}(p^{m-d}-1)(p^{m-2d}+1)(p^n-1)\big/\big((p^d+1)(p^{2d}-1)\big)$
0	$(p^n-1)(p^{3m-d}-p^{3m-2d}+p^{3m-3d}-p^{3m-4d}+p^{3m-5d}$ $+p^{n-d}-2p^{n-2d}+p^{n-3d}-p^{n-4d}+1)$
p^n	1

where $1\leq j\leq p-1$.

Proof. see **Appendix C.** ☐

Remark. Case (i) is exactly Proposition 6 in [30].

In order to give the correlation distribution among the sequences in $\mathcal{F}$, we need the following lemma (see [30], Lemma 5).

Lemma 7. *For any given $\gamma \in \mathbb{F}_q^*$, when (α, β) runs through $\mathbb{F}_{p^m} \times \mathbb{F}_q$, the distribution of $S(\alpha, \beta, \gamma)$ is the same as $S(\alpha, \beta, 1)$.*

As a consequence of Theorem 1, Theorem 3 and Lemma 7, we could give the correlation distribution amidst the sequences in $\mathcal{F}$.

Theorem 4. *The collection $\mathcal{F}$ defined in (5) is a family of p^{3m} p-ary sequences with period $q-1$. Its correlation distribution is given as follows.*

(i). If $d' = d$ is odd, then

values	*multiplicity*
$p^m - 1$	$p^{3m+d}(p^m+1)\left(p^{m-1}(p^m+p-1)(p^n-2)+1\right) \big/ \left(2(p^d+1)\right)$
$-p^m - 1$	$p^{3m+d}\left(p^{m-1}(p^m-p+1)(p^n-2)+1\right)\left(p^n-2p^{n-d}+1\right) \big/ \left(2(p^d-1)(p^m+1)\right)$
$\zeta_p^j p^m - 1$	$p^{2n+d-1}(p^n-2)(p^n-1) \big/ \left(2(p^d+1)\right)$
$-\zeta_p^j p^m - 1$	$p^{2n+d-1}(p^n-2)(p^n-2p^{n-d}+1) \big/ \left(2(p^d-1)\right)$
$\varepsilon\sqrt{p^*}p^{m+\frac{d-1}{2}} - 1$	$\frac{1}{2}p^{2n-d}\left(p^{n-d-1}(p^n-2)+1\right)$
$\varepsilon\zeta_p^j\sqrt{p^*}p^{m+\frac{d-1}{2}} - 1$	$\frac{1}{2}p^{5m-\frac{3d+1}{2}}\left(p^{m-\frac{d+1}{2}}+\varepsilon\left(\frac{-j}{p}\right)\right)(p^n-2)$
$-p^{\frac{m}{2}+d} - 1$	$p^{3m}(p^{m-d}-1)\left(p^{m-d-1}(p^n-2)(p^{m-d}-p+1)+1\right) \big/ \left(p^{2d}-1\right)$
$-\zeta_p^j p^{m+d} - 1$	$p^{2n-d-1}(p^{m-d}-1)(p^n-2)(p^{m-d}+1) \big/ \left(p^{2d}-1\right)$
-1	$p^{3m}(p^n-2)(p^{3m-d}-p^{3m-2d}+p^{3m-3d}-p^{n-2d}+1)$
$p^n - 1$	p^{3m}

where $1 \le j \le p-1$ and $\varepsilon = \pm 1$.

(ii). If $d' = d$ is even, then

values	*multiplicity*
p^m-1	$p^{3m+d}(p^m+1)\left(p^{m-1}(p^m+p-1)(p^n-1)+1\right)/\left(2(p^d+1)\right)$
$-p^m-1$	$p^{3m+d}\left(p^{m-1}(p^m-p+1)(p^n-2)+1\right)\left(p^n-2p^{n-d}+1\right)/\left(2(p^d-1)(p^m+1)\right)$
$\zeta_p^j p^m-1$	$p^{2n+d-1}(p^n-2)(p^n-1)/\left(2(p^d+1)\right)$
$-\zeta_p^j p^m-1$	$p^{2n+d-1}(p^n-2)(p^n-2p^{n-d}+1)/\left(2(p^d-1)\right)$
$\varepsilon p^{m+\frac{d}{2}}$	$\frac{1}{2}p^{2n-d}\left(p^{m-\frac{d}{2}-1}(p^{m-\frac{d}{2}}+\varepsilon(p-1))(p^n-2)+1\right)$
$\varepsilon\zeta_p^j p^{m+\frac{d}{2}}$	$\frac{1}{2}p^{5m-\frac{3d}{2}-1}(p^{m-\frac{d}{2}}-\varepsilon)(p^n-2)$
$-p^{\frac{m}{2}+d}-1$	$p^{3m}(p^{m-d}-1)\left(p^{m-d-1}(p^n-2)(p^{m-d}-p+1)+1\right)/\left(p^{2d}-1\right)$
$-\zeta_p^j p^{m+d}-1$	$p^{2n-d-1}(p^{n-2d}-1)(p^n-2)/\left(p^{2d}-1\right)$
-1	$p^{3m}(p^n-2)(p^{3m-d}-p^{3m-2d}+p^{3m-3d}-p^{n-2d}+1)$
p^n-1	p^{3m}

where $1\le j\le p-1$ *and* $\varepsilon=\pm1$.

(iii). If $d'=2d$, *then*

values	*multiplicity*
$-p^m-1$	$p^{3m+3d}(p^{m-1}(p^m-p+1)(p^n-2)+1)(p^n-p^{n-2d}-p^{n-3d}+$ $p^m-p^{m-d}+1)/(p^d+1)(p^{2d}-1)(p^m+1)$
$-\zeta_p^j p^m-1$	$p^{2n+3d-1}(p^n-2)(p^n-p^{n-2d}-p^{n-3d}+p^m-p^{m-d}+1)/(p^d+1)(p^{2d}-1)$
$p^{m+d}-1$	$p^{3m+d}\left(p^{m-d-1}(p^{m-d}+p-1)(p^n-2)+1\right)(p^m+p^{m-d}+p^{m-2d}+1)/(p^d+1)^2$
$\zeta_p^j p^{m+d}-1$	$p^{2n-1}(p^n-2)(p^{m-d}-1)(p^m+p^{m-d}+p^{m-2d}+1)/(p^d+1)^2$
$-p^{m+2d}-1$	$p^{3m}(p^{m-d}-1)\left(p^{m-2d-1}(p^{m-2d}-p+1)(p^n-2)+1\right)/\left((p^d+1)(p^{2d}-1)\right)$
$-\zeta_p^j p^{m+2d}-1$	$p^{2n-2d-1}(p^{m-d}-1)(p^{m-2d}+1)(p^n-2)/\left((p^d+1)(p^{2d}-1)\right)$
-1	$p^{3m}(p^n-2)(p^{3m-d}-p^{3m-2d}+p^{3m-3d}-p^{3m-4d}+p^{3m-5d}$ $+p^{n-d}-2p^{n-2d}+p^{n-3d}-p^{n-4d}+1)$
p^n-1	p^{3m}

where $1\le j\le p-1$.

Proof. see **Appendix C.** $\square$

Remark. The case (i) has been shown in [30], Prop. 6.

Recall that $\mathcal{C}_2$ is the cyclic code over $\mathbb{F}_{p^t}$ with parity-check polynomial $h_1(x)h_2(x)h_3(x)$ where $h_1(x)$, $h_2(x)$ and $h_3(x)$ are the minimal polynomials of π^{-1}, $\pi^{-(p^k+1)}$ and $\pi^{-(p^m+1)}$ respectively. Here we are ready to determine the weight distribution of $\mathcal{C}_2$.

Theorem 5. *The weight distribution* $\{A_0, A_1, \cdots, A_{q-1}\}$ *of the cyclic code* $\mathcal{C}_2$ *over* $\mathbb{F}_{p^t}$ $(p \geq 3)$ *with length* $q-1$ *and* $\dim_{\mathbb{F}_{p^t}} \mathcal{C}_1 = \frac{5}{2} n_0$ *is shown as following.*

(i). If $d' = d$ *and* d/t *is odd, then*

i	A_i
$(p^t-1)(p^{n-t}-p^{m-t})$	$p^{m+d-t}(p^m+p^t-1)(p^m-1)(p^m+1)^2 / \big(2(p^d+1)\big)$
$(p^t-1)(p^{n-t}+p^{m-t})$	$p^{m+d-t}(p^m-p^t+1)(p^m-1)(p^n-2p^{n-d}+1) / \big(2(p^d-1)\big)$
$(p^t-1)p^{n-t}+p^{m-t}$	$p^{m+d-t}(p^t-1)(p^n-1)^2 / \big(2(p^d+1)\big)$
$(p^t-1)p^{n-t}-p^{m-t}$	$p^{m+d-t}(p^t-1)(p^n-1)(p^n-2p^{n-d}+1) / \big(2(p^d-1)\big)$
$(p^t-1)p^{n-t}-p^{m+\frac{d-t}{2}}$	$\frac{1}{2}p^{m-d}(p^t-1)(p^{n-d-t}+p^{\frac{n-d-t}{2}})(p^n-1)$
$(p^t-1)p^{n-t}+p^{m+\frac{d-t}{2}}$	$\frac{1}{2}p^{m-d}(p^t-1)(p^{n-d-t}-p^{\frac{n-d-t}{2}})(p^n-1)$
$(p^t-1)(p^{n-t}+p^{m+d-t})$	$p^{m-d-t}(p^{m-d}-1)(p^{m-d}-p^t+1)(p^n-1) / \big(p^{2d}-1\big)$
$(p^t-1)p^{n-t}-p^{m+d-t}$	$p^{m-d-t}(p^t-1)(p^{n-2d}-1)(p^n-1) / \big(p^{2d}-1\big)$
$(p^t-1)p^{n-t}$	$(p^n-1)(p^{3m-d}-p^{3m-2d}+p^{3m-3d}+p^{3m-2d-t}-p^{n-2d}+1)$
0	1

(ii). If $d' = d$ *and* d/t *is even, then*

i	A_i
$(p^t-1)(p^{n-t}-p^{m-t})$	$p^{m+d-t}(p^m+p^t-1)(p^m-1)(p^m+1)^2\big/\big(2(p^d+1)\big)$
$(p^t-1)(p^{n-t}+p^{m-t})$	$p^{m+d-t}(p^m-p^t+1)(p^m-1)(p^n-2p^{n-d}+1)\big/\big(2(p^d-1)\big)$
$(p^t-1)p^{n-t}+p^{m-t}$	$p^{m+d-t}(p^t-1)(p^n-1)^2\big/\big(2(p^d+1)\big)$
$(p^t-1)p^{n-t}-p^{m-t}$	$p^{m+d-t}(p^t-1)(p^n-1)(p^n-2p^{n-d}+1)\big/\big(2(p^d-1)\big)$
$(p^t-1)(p^{n-t}-p^{m+\frac{d}{2}-t})$	$\frac{1}{2}p^{m-d}(p^{n-d-t}+(p^t-1)p^{m-t-\frac{d}{2}})(p^n-1)$
$(p^t-1)(p^{n-t}+p^{m+\frac{d}{2}-t})$	$\frac{1}{2}p^{m-d}(p^{n-d-t}-(p^t-1)p^{m-t-\frac{d}{2}})(p^n-1)$
$(p^t-1)p^{n-t}-p^{m+\frac{d}{2}-t}$	$\frac{1}{2}p^{m-d}(p^t-1)(p^{n-d-t}+p^{m-t-\frac{d}{2}})(p^n-1)$
$(p^t-1)p^{n-t}+p^{m+\frac{d}{2}-t}$	$\frac{1}{2}p^{m-d}(p^t-1)(p^{n-d-t}-p^{m-t-\frac{d}{2}})(p^n-1)$
$(p^t-1)(p^{n-t}+p^{m+d-t})$	$p^{m-d-t}(p^{m-d}-1)(p^{m-d}-p^t+1)(p^n-1)\big/\big(p^{2d}-1\big)$
$(p^t-1)p^{n-t}-p^{m+d-t}$	$p^{m-d-t}(p^t-1)(p^{n-2d}-1)(p^n-1)\big/\big(p^{2d}-1\big)$
$(p^t-1)p^{n-t}$	$(p^n-1)(p^{3m-d}-p^{3m-2d}+p^{3m-3d}-p^{n-2d}+1)$
0	1

(iii). If $d'=2d$, then

values	*multiplicity*
$(p^t-1)(p^{n-t}+p^{m-t})$	$p^{m+3d-t}(p^m-p^t+1)(p^m-1)(p^n-p^{n-2d}-p^{n-3d}$ $+p^m-p^{m-d}+1)\big/\big((p^d+1)(p^{2d}-1)\big)$
$(p^t-1)p^{n-t}-p^{m-t}$	$p^{m+3d-t}(p^t-1)(p^n-1)(p^n-p^{n-2d}-p^{n-3d}$ $+p^m-p^{m-d}+1)\big/\big((p^d+1)(p^{2d}-1)\big)$
$(p^t-1)(p^{n-t}-p^{m+d-t})$	$p^{m-t}(p^{m-d}+p^t-1)(p^n-1)(p^m+p^{m-d}+p^{m-2d}+1)\big/(p^d+1)^2$
$(p^t-1)p^{n-t}+p^{m+d-t}$	$p^{m-t}(p^t-1)(p^{m-d}-1)(p^n-1)(p^m+p^{m-d}+p^{m-2d}+1)\big/(p^d+1)^2$
$(p^t-1)(p^{n-t}+p^{m+2d-t})$	$p^{m-2d-t}(p^{m-2d}-p^t+1)(p^{m-d}-1)(p^n-1)\big/\big((p^d+1)(p^{2d}-1)\big)$
$(p^t-1)p^{n-t}-p^{m+2d-t}$	$p^{m-2d-t}(p^t-1)(p^{m-2d}-1)(p^{m-d}-1)(p^n-1)\big/\big((p^d+1)(p^{2d}-1)\big)$
$(p^t-1)p^{n-t}$	$(p^n-1)(p^{3m-d}-p^{3m-2d}+p^{3m-3d}-p^{3m-4d}+p^{3m-5d}$ $+p^{n-d}-2p^{n-2d}+p^{n-3d}-p^{n-4d}+1)$
0	1

Proof. see **Appendix C.** ☐

Remark. The case (i) with $t = 1$ has been shown in [30], Theorem 1.

5 Appendix A

We need to introduce some results to prove Lemma 2.

Lemma 8. *(see Bluher [1], Theorem 5.4 and 5.6) Let $g(z) = z^{p^h+1} - bz + b$ with $b \in \mathbb{F}_{p^l}^*$. Then the number of the solutions to $g(z) = 0$ in $\mathbb{F}_{p^l}$ is 0, 1, 2 or $p^{\gcd(h,l)} + 1$. Moreover, the number of $b \in \mathbb{F}_{p^l}^*$ such that $g(z) = 0$ has unique solution in $\mathbb{F}_{p^l}$ is $p^{l-\gcd(h,l)}$ and if z_0 is the unique solution, then $(z_0 - 1)^{\frac{p^l-1}{p^{\gcd(h,l)}-1}} = 1$.*

The following lemma has been proven in [1] and [30]. We will give some of the details for self-containing.

Lemma 9. *Let $\psi_{\alpha,\beta}(z) = \beta^{p^{n-k}} z^{p^{m-k}+1} + \alpha z + \beta$ with $\alpha \in \mathbb{F}_{p^m}^*, \beta \in \mathbb{F}_q^*$. Then*

(i). $\psi_{\alpha,\beta}(z) = 0$ has either $0, 1, 2$ or $p^{d'} + 1$ solutions in $\mathbb{F}_q$.

(ii). If z_1, z_2 are two solutions of $\psi_{\alpha,\beta}(z) = 0$ in $\mathbb{F}_q$, then $z_1 z_2$ is $(p^d - 1)$-th power in $\mathbb{F}_q$.

(iii). If $\psi_{\alpha,\beta}(z) = 0$ has $p^{d'} + 1$ solutions in $\mathbb{F}_q$, then for any two solutions z_1 and z_2, we have z_1/z_2 is a $(p^{d'} - 1)$-th power in $\mathbb{F}_q$.

(iv). If $\psi_{\alpha,\beta}(z) = 0$ has exactly one solution in $\mathbb{F}_q$, then it is a $(p^d - 1)$-th power in $\mathbb{F}_q$.

Proof. (i). By scaling $y = -\frac{\alpha}{\beta} z$ and $b = \frac{\alpha^{p^{m-k}+1}}{\beta^{p^{m-k}(p^m+1)}}$, we can rewrite the equation $\psi_{\alpha,\beta}(z) = 0$ as

$$y^{p^{m-k}+1} - by + b = 0. \tag{13}$$

Since $b \in \mathbb{F}_q^*$ and $\gcd(m - k, n) = \gcd(m - k, 2k) = d'$, then the result follows from Lemma 8.

(ii). See [30], Prop.1 (2).

(iii). Denote by $y_i = -\frac{\alpha}{\beta} z_i$ for $i = 1, 2$. Since $\gcd(n, m-k) = d'$, from [1], Theorem 4.6 (iv) we get $(y_1/y_2)^{\frac{q-1}{p^{d'}-1}} = 1$ which is equivalent to $(z_1/z_2)^{\frac{q-1}{p^{d'}-1}} = 1$.

(iv). See [30], Prop.1 (3).

$\square$

Proof of Lemma 2: (i). For $Y = (y_1, \cdots, y_s) \in \mathbb{F}_{q_0}^s$, $y = y_1 v_1 + \cdots + y_s v_s \in \mathbb{F}_q$, we know that

$$F_{\alpha,\beta}(X+Y) - F_{\alpha,\beta}(X) - F_{\alpha,\beta}(Y) = 2XH_{\alpha,\beta}Y^T \tag{14}$$

is equal to

$$f_{\alpha,\beta}(x+y) - f_{\alpha,\beta}(x) - f_{\alpha,\beta}(y) = \mathrm{Tr}_d^n\left(y(\alpha x^{p^m} + \beta x^{p^k} + \beta^{p^{n-k}} x^{p^{n-k}})\right) \tag{15}$$

since $\mathrm{Tr}_d^m(\alpha x^{p^m} y + \alpha x y^{p^m}) = \mathrm{Tr}_d^n(\alpha x^{p^m} y)$.

Let

$$\phi_{\alpha,\beta}(x) = \alpha x^{p^m} + \beta x^{p^k} + \beta^{p^{n-k}} x^{p^{n-k}}. \tag{16}$$

Therefore,

$$\begin{aligned} r_{\alpha,\beta} = r &\Leftrightarrow \text{the number of common solutions of } XH_{\alpha,\beta}Y^T = 0 \text{ for all } Y \in \mathbb{F}_{q_0}^s \text{ is } q_0^{s-r}, \\ &\Leftrightarrow \text{the number of common solutions of } \mathrm{Tr}_d^n\left(y \cdot \phi_{\alpha,\beta}(x)\right) = 0 \text{ for all } y \in \mathbb{F}_q \text{ is } q_0^{s-r}, \\ &\Leftrightarrow \phi_{\alpha,\beta}(x) = 0 \text{ has } q_0^{s-r} \text{ solutions in } \mathbb{F}_q. \end{aligned}$$

Since $\phi_{\alpha,\beta}(x)$ is a p^d-linearized polynomial, then the set of the zeroes to $\phi_{\alpha,\beta}(x) = 0$ in $\mathbb{F}_{p^n}$, say V, forms an $\mathbb{F}_{p^d}$-vector space.

If $\alpha = 0$ and $\beta \neq 0$, $\phi_{\alpha,\beta}(x) = 0$ becomes $\beta x^{p^k} + \beta^{p^{n-k}} x^{p^{n-k}} = 0$ and then $\beta^{p^k} x^{p^{2k}} + \beta x = 0$. In this case (16) has 1 or $p^{d'}$ solutions according to $-\beta^{1-p^k}$ is $(p^{d'}-1)$-th power in $\mathbb{F}_q$ or not. Hence $r_{0,\beta} = s$ or $s - d'/d$. If $\alpha \neq 0$ and $\beta = 0$, then $\phi_{\alpha,\beta}(x) = 0$ has unique solution $x = 0$ and as a consequence $r_{\alpha,0} = s$.

In the following we assume $\alpha\beta \neq 0$, we need to consider the nonzero solutions of $\phi_{\alpha,\beta}(x) = 0$. By substituting $z = x^{p^k(p^{m-k}-1)}$ we get

$$\psi_{\alpha,\beta}(z) = \beta^{p^{n-k}} z^{p^{m-k}+1} + \alpha z + \beta = 0. \tag{17}$$

From Lemma 8, $\psi_{\alpha,\beta}(z) = 0$ has either $0, 1, 2$ or $p^{d'}+1$ solutions in $\mathbb{F}_q$. In the case $d' = d$, by Lemma 9, if $\psi_{\alpha,\beta}(z) = 0$ has at least two solutions in $\mathbb{F}_q$, then all or none of the solutions are (p^d-1)-th power. Then $\psi_{\alpha,\beta}(x) = 0$ has

$0, p^d-1, 2(p^d-1)$ or $(p^d+1)(p^d-1)$ nonzero solutions. Take the solution $x=0$ in consideration, since $2p^d-1$ is not a p^d-th power, then it is impossible and we get the result.

In the case $d'=2d$, the argument is almost the same except $\psi_{\alpha,\beta}(z)=0$ has two solutions z_1, z_2. If none, one or two of the solutions is $(p^{2d}-1)$-th power, then $\phi_{\alpha,\beta}(x)=0$ has 1, $p^{2d}-1$ or $2(p^{2d}-1)$ nonzero solutions. But $2p^{2d}-1$ is not a p^d-th power. Then the result follows.

In the case $d'=d$, if $\psi_{\alpha,\beta}(z)=0$ has unique solution $z_0\in\mathbb{F}_q$, then it is also the unique solution in $\mathbb{F}_{p^m}$ and the converse is also valid, since $b\in\mathbb{F}_{p^m}$ and the solutions of $\psi_{\alpha,\beta}(z)=0$ in $\mathbb{F}_q\Big\backslash\mathbb{F}_{p^m}$ take on pairs $(z_0, z_0^{p^m})$. By [1], Theorem 5.6, the number of $b\in\mathbb{F}_{p^m}^*$ such that $\psi_{\alpha,\beta}(z)=0$ has unique solution in $\mathbb{F}_{p^m}$ is p^{m-d}. For fixed b and $\alpha\in\mathbb{F}_{p^m}^*$, the number of $\beta\in\mathbb{F}_q^*$ satisfying $b=\frac{\alpha^{p^{m-k}+1}}{\beta^{p^{m-k}(p^m+1)}}$ is p^m+1. Hence $n_1=p^{m-d}(p^m-1)(p^m+1)=p^{m-d}(p^n-1)$. $\square$

Proof of Lemma 3: (i). We observe that

$$\begin{aligned}\sum_{\alpha\in\mathbb{F}_{p^m},\beta\in\mathbb{F}_q} T(\alpha,\beta) &= \sum_{\alpha\in\mathbb{F}_{p^m},\beta\in\mathbb{F}_q}\sum_{x\in\mathbb{F}_q}\zeta_p^{\mathrm{Tr}_1^m(\alpha x^{p^m+1})+\mathrm{Tr}_1^n(\beta x^{p^k+1})}\\ &= \sum_{x\in\mathbb{F}_q}\sum_{\alpha\in\mathbb{F}_{p^m}}\zeta_p^{\mathrm{Tr}_1^m(\alpha x^{p^m+1})}\sum_{\beta\in\mathbb{F}_q}\zeta_p^{\mathrm{Tr}_1^n(\beta x^{p^k+1})} = q\cdot\sum_{\substack{\alpha\in\mathbb{F}_{p^m}\\ x=0}}\zeta_p^{\mathrm{Tr}_1^m(\alpha x^{p^m+1})} = p^{3m}.\end{aligned}$$

(ii). We can calculate

$$\begin{aligned}\sum_{\alpha\in\mathbb{F}_{p^m},\beta\in\mathbb{F}_q} T(\alpha,\beta)^2 &= \sum_{x,y\in\mathbb{F}_q}\sum_{\alpha\in\mathbb{F}_{p^m}}\zeta_p^{\mathrm{Tr}_1^m\left(\alpha\left(x^{p^m+1}+y^{p^m+1}\right)\right)}\sum_{\beta\in\mathbb{F}_q}\zeta_p^{\mathrm{Tr}_1^n\left(\beta\left(x^{p^k+1}+y^{p^k+1}\right)\right)}\\ &= M_2\cdot p^{3m}\end{aligned}$$

where M_2 is the number of solutions to the equation

$$\left\{\begin{array}{l} x^{p^m+1}+y^{p^m+1}=0\\ x^{p^k+1}+y^{p^k+1}=0\end{array}\right. \tag{18}$$

If $xy=0$ satisfying (18), then $x=y=0$. Otherwise $(x/y)^{p^m+1}=(x/y)^{p^k+1}=-1$ which yields that $(x/y)^{p^{m-k}-1}=1$. Denote by $x=ty$. Since $\gcd(m-k,n)=d'$, then $t\in\mathbb{F}_{p^{d'}}^*$.

- If $d'=d$, then $t\in\mathbb{F}_{p^d}^*$ and (18) is equivalent to $x^2+y^2=0$. Hence $t^2=-1$. There are two or none of $t\in\mathbb{F}_{p^d}^*$ satisfying $t^2=-1$ depending on $p^d\equiv 1$

(mod 4) or $p^d \equiv 3 \pmod 4$. Therefore

$$M_2 = \begin{cases} 1 + 2(q-1) = 2q-1, & \text{if } p^d \equiv 1 \pmod 4 \\ 1, & \text{if } p^d \equiv 3 \pmod 4. \end{cases}$$

- If $d' = 2d$, then by (11) we get (18) is equivalent to $x^{p^d+1} + y^{p^d+1} = 0$. Then we have $t^{p^d+1} = -1$ which has $p^d + 1$ solutions in $\mathbb{F}_{p^{d'}}^*$. Therefore

$$M_2 = (p^d+1)(p^n-1) + 1 = p^{n+d} + p^n - p^d.$$

(iii). See [30], Prop.4 iii).□

Remark. For the case $d' = 2d$, $\sum_{\alpha,\beta \in \mathbb{F}_q} T(\alpha,\beta)^3$ can also be determined, but we do not need this result.

Proof of Lemma 4: We get that

$$\begin{aligned} qN &= \sum_{\omega \in \mathbb{F}_q} \sum_{x,y \in \mathbb{F}_q} \zeta_p^{\mathrm{Tr}_1^n\left(\omega\left(\frac{1}{2}\alpha x^{p^m+1} + \beta x^{p^k+1} - y^{p^d} + y\right)\right)} \\ &= q^2 + \sum_{\omega \in \mathbb{F}_q^*} \sum_{x \in \mathbb{F}_q} \zeta_p^{\mathrm{Tr}_1^n\left(\omega\left(\frac{1}{2}\alpha x^{p^m+1} + \beta x^{p^k+1}\right)\right)} \sum_{y \in \mathbb{F}_q} \zeta_p^{\mathrm{Tr}_1^n\left(y^{p^d}\left(\omega^{p^d} - \omega\right)\right)} \\ &= q^2 + q \sum_{\omega \in \mathbb{F}_{q_0}^*} \sum_{x \in \mathbb{F}_q} \zeta_p^{\mathrm{Tr}_1^n\left(\omega\left(\frac{1}{2}\alpha x^{p^m+1} + \beta x^{p^k+1}\right)\right)} \\ &= q^2 + q \sum_{\omega \in \mathbb{F}_{q_0}^*} \sum_{x \in \mathbb{F}_q} \zeta_p^{\mathrm{Tr}_1^m\left(\omega\alpha x^{p^m+1}\right) + \mathrm{Tr}_1^n\left(\omega\beta x^{p^k+1}\right)} \\ &= q^2 + q \sum_{\omega \in \mathbb{F}_{q_0}^*} \sum_{x \in \mathbb{F}_q} T(\omega\alpha, \omega\beta) \end{aligned}$$

where the 3-rd equality follows from that the inner sum is zero unless $\omega^{p^d} - \omega = 0$, i.e. $\omega \in \mathbb{F}_{q_0}$ and the 4-th equality follows from $\frac{1}{2}\omega\alpha x^{p^m+1} \in \mathbb{F}_{p^m}$.

For any $\omega \in \mathbb{F}_{q_0}^*$, by (10) we have $F_{\omega\alpha,\omega\beta}(X) = \omega \cdot F_{\alpha,\beta}(X)$, $H_{\omega\alpha,\omega\beta} = \omega \cdot H_{\alpha,\beta}$ and $r_{\omega\alpha,\omega\beta} = r_{\alpha,\beta}$. From Lemma 1 (i) we know that

$$T(\omega\alpha, \omega\beta) = \sum_{X \in \mathbb{F}_{q_0}^s} \zeta_p^{\mathrm{Tr}_1^d(XH_{\omega\alpha,\omega\beta}X^T)} = \eta_0(\omega)^{r_{\alpha,\beta}} T(\alpha,\beta). \tag{19}$$

In the case $d' = 2d$, by Lemma 2ii) we get that $r_{\alpha,\beta}$ is even. Hence $T(\omega\alpha,\omega\beta) = T(\alpha,\beta)$ for any $\omega \in \mathbb{F}_{p^t}^*$ and $N = q + (p^d-1)T(\alpha,\beta)$. □

6 Appendix B

Proof of Theorem 1:

Define

$$N_i = \{(\alpha,\beta) \in \mathbb{F}_{p^m} \times \mathbb{F}_q \backslash \{(0,0)\} \, | r_{\alpha,\beta} = s - i\}.$$

Then $n_i = \left|N_i\right|$.

According to Lemma 1 (setting $F(X) = XH_{\alpha,\beta}X^T = \mathrm{Tr}_d^m(\alpha x^{p^m+1}) + \mathrm{Tr}_d^n(\beta x^{p^k+1})$), we define that for $\varepsilon = \pm 1$ and $0 \le i \le s-1$,

$$N_{i,\varepsilon} = \begin{cases} \left\{(\alpha,\beta) \in \mathbb{F}_{p^m} \times \mathbb{F}_q \backslash \{(0,0)\} \,\middle|\, T(\alpha,\beta) = \varepsilon p^{\frac{m+id}{2}}\right\} & \text{if } m+id \text{ is even },\\ \left\{(\alpha,\beta) \in \mathbb{F}_{p^m} \times \mathbb{F}_q \backslash \{(0,0)\} \,\middle|\, T(\alpha,\beta) = \varepsilon \sqrt{p^*} p^{\frac{m+id-1}{2}}\right\} & \text{if } m+id \text{ is odd} \end{cases}$$

where $p^* = (-1)^{\frac{p-1}{2}} p$ and $n_{i,\varepsilon} = |N_{i,\varepsilon}|$. Then $N_i = N_{i,1} \bigcup N_{i,-1}$ and $n_i = n_{i,1} + n_{i,-1}$.

(i). For the case $d' = d$, by Lemma 2 we have

$$n_{1,1} + n_{1,-1} = p^{m-d}(p^n - 1). \tag{20}$$

Choose an element $\omega \in \mathbb{F}_{q_0}^*$ such that $\eta_0(\omega) = -1$. For any $(\alpha,\beta) \in N_{1,\varepsilon}$, since $s-1$ is odd, by (19) we get $T(\omega\alpha,\omega\beta) = -T(\alpha,\beta)$. Then the map $(\alpha,\beta) \mapsto (\omega\alpha,\omega\beta)$ give a 1-to-1 correspondence from $N_{1,1}$ to $N_{1,-1}$ Combining (20) one has

$$n_{1,1} = n_{1,-1} = \frac{1}{2} p^{m-d}(p^n - 1). \tag{21}$$

Moreover, from Lemma 3 and (21) we have

$$(n_{0,1} - n_{0,-1}) + p^d \,(n_{2,1} - n_{2,-1}) = p^m(p^m - 1) \tag{22}$$

$$(n_{0,1} + n_{0,-1}) + p^{2d} \,(n_{2,1} + n_{2,-1}) = p^n(p^m - 1) \tag{23}$$

$$(n_{0,1} - n_{0,-1}) + p^{3d} \,(n_{2,1} - n_{2,-1}) = p^d(p^m - 1)(-p^{n-d} + p^m + 1). \tag{24}$$

In addition, by Lemma 2 and (21) we have

$$(n_{0,1} + n_{0,-1}) + (n_{2,1} + n_{2,-1}) = (p^m - 1)(p^n - p^{n-d} + p^m - p^{m-d} + 1). \tag{25}$$

Combining (22)–(25), together with (21) we get the result.

(ii). For the case $d' = 2d$, by Lemma 5 we have

$$n_{0,1} = n_{2,-1} = n_{4,1} = 0. \tag{26}$$

Combining Lemma 2, Lemma 3 and (26) we have

$$n_{0,-1} + n_{2,1} + n_{4,-1} = p^{3m} - 1 \tag{27}$$

$$-n_{0,-1} + p^d \cdot n_{2,1} - p^{2d} \cdot n_{4,-1} = p^m(p^m - 1) \tag{28}$$

$$n_{0,-1} + p^{2d} \cdot n_{2,1} + p^{4d} \cdot n_{4,-1} = p^m(p^{n+d} + p^n - p^m - p^d). \tag{29}$$

Solving the system of equations consisting of (27)–(29) yields the result. $\square$

Proof of Theorem 2: From (1) we know that for each non-zero codeword $c(\alpha, \beta) = (c_0, \cdots, c_{l-1})$ $(l = q-1, c_i = \mathrm{Tr}_1^m(\alpha\pi^{(p^m+1)i}) + \mathrm{Tr}_1^n(\beta\pi^{(p^k+1)i}), 0 \le i \le l-1, \text{and } (\alpha, \beta) \in \mathbb{F}_{p^m} \times \mathbb{F}_q)$, the Hamming weight of $c(\alpha, \beta)$ is

$$w_H\left(c(\alpha, \beta)\right) = p^{m-t}(p^t - 1) - \frac{1}{p^t} \cdot R(\alpha, \beta) \tag{30}$$

where

$$R(\alpha, \beta) = \sum_{a \in \mathbb{F}_{p^t}^*} T(a\alpha, a\beta) = T(\alpha, \beta) \sum_{a \in \mathbb{F}_{p^t}^*} \eta_0(a)^{r_{\alpha,\beta}}$$

by Lemma 1 (i).

Let η' be the quadratic (multiplicative) character on $\mathbb{F}_q$. Then we have

(1). if d/t or $r_{\alpha,\beta}$ is even, then $\sum\limits_{a \in \mathbb{F}_{p^t}^*} \eta_0(a)^{r_{\alpha,\beta}} = \sum\limits_{a \in \mathbb{F}_{p^t}^*} 1 = p^t - 1$ and $R(\alpha, \beta) = (p^t - 1)T(\alpha, \beta)$.

(2). if d/t and $r_{\alpha,\beta}$ are both odd, then $\sum\limits_{a \in \mathbb{F}_{p^t}^*} \eta_0(a)^{r_{\alpha,\beta}} = \sum\limits_{a \in \mathbb{F}_{p^t}^*} \eta'(a) = 0$ and $R(\alpha, \beta) = 0$.

Thus the weight distribution of $\mathcal{C}_1$ can be derived from Theorem 1 and (30) directly. For example, if d/t is odd and $d' = d$, then

(1). if $r_{\alpha,\beta} = s$ and $T(\alpha, \beta) = p^m$, then $w_H(c(\alpha, \beta)) = (p^t - 1)(p^{n-t} - p^{m-t})$.

(2). if $r_{\alpha,\beta} = s$ and $T(\alpha, \beta) = -p^m$, then $w_H(c(\alpha, \beta)) = (p^t - 1)(p^{n-t} + p^{m-t})$.

(3). if $r_{\alpha,\beta} = s - 1$, then $w_H(c(\alpha, \beta)) = (p^t - 1)p^{n-t}$.

(4). if $r_{\alpha,\beta} = s - 2$ and $T(\alpha, \beta) = -p^{m+d}$, then $w_H(c(\alpha, \beta)) = (p^t - 1)(p^{n-t} + p^{m+d-t})$.

$\square$

7 Appendix C

Proof of Lemma 6:

Define $n(\alpha, \beta, a)$ to be the number of $\gamma \in \mathbb{F}_q$ satisfying (i) and (ii). From (10) we know that $XH_{\alpha,\beta}X^T = \mathrm{Tr}_d^m(\alpha x^{p^m+1}) + \mathrm{Tr}_d^n(\beta x^{p^k+1})$. Combining (2), (14) and (15) we can get

$$\begin{aligned} 2XH_{\alpha,\beta} + A_\gamma = 0 &\Leftrightarrow\ 2XH_{\alpha,\beta}Y^T + A_\gamma Y^T = 0 \text{ for all } Y \in \mathbb{F}_{q_0}^s \\ &\Leftrightarrow\ \mathrm{Tr}_d^n\left(y\phi_{\alpha,\beta}(x)\right) + \mathrm{Tr}_d^n(\gamma y) = 0 \text{ for all } y \in \mathbb{F}_q \\ &\Leftrightarrow\ \mathrm{Tr}_d^n\left(y(\phi_{\alpha,\beta}(x) + \gamma)\right) = 0 \text{ for all } y \in \mathbb{F}_q \\ &\Leftrightarrow \phi_{\alpha,\beta}(x) + \gamma = 0. \end{aligned} \tag{31}$$

Let x_0, x_0' be two distinct solutions of (i) (if exists). We can get $x_0 = X_0 \cdot V^T$ and $x_0' = X_0' \cdot V^T$ with $X_0, X_0' \in \mathbb{F}_{q_0}^s$ and $V = (v_1, \cdots, v_n)$. Define $\Delta X_0 = X_0' - X_0$ and $\Delta x_0 = x_0' - x_0 = X_0 \cdot V^T$. Then

$$\phi_{\alpha,\beta}(x_0) + \gamma = \phi_{\alpha,\beta}(x_0') + \gamma = 0$$

gives us

$$2X_0H_{\alpha,\beta} + A_\gamma = 2X_0'H_{\alpha,\beta} + A_\gamma = 0$$

and hence

$$\Delta X_0 \cdot H_{\alpha,\beta} = 0.$$

It follows that

$$\begin{aligned} X_0' \cdot H_{\alpha,\beta} \cdot {X_0'}^T &= (X_0 + \Delta X_0) \cdot H_{\alpha,\beta} \cdot (X_0 + \Delta X_0)^T \\ &= X_0 H_{\alpha,\beta} X_0^T + \Delta X_0 \cdot H_{\alpha,\beta} \cdot (\Delta X_0 + 2X_0) = X_0 H_{\alpha,\beta} X_0^T. \end{aligned}$$

Therefore

$$\begin{aligned} &\mathrm{Tr}_t^m(\alpha {x_0'}^{p^m+1}) + \mathrm{Tr}_t^n(\beta {x_0'}^{p^k+1}) = \mathrm{Tr}_t^d\left(\mathrm{Tr}_t^m(\alpha {x_0'}^{p^m+1}) + \mathrm{Tr}_t^n(\beta {x_0'}^{p^k+1})\right) = \mathrm{Tr}_t^d\left(X_0' \cdot H_{\alpha,\beta} \cdot {X_0'}^T\right) \\ &= \mathrm{Tr}_t^d\left(X_0 H_{\alpha,\beta} {X_0}^T\right) = \mathrm{Tr}_t^d\left(\mathrm{Tr}_t^m(\alpha {x_0}^{p^m+1}) + \mathrm{Tr}_t^n(\beta {x_0}^{p^k+1})\right) = \mathrm{Tr}_t^m(\alpha {x_0}^{p^m+1}) + \mathrm{Tr}_t^n(\beta {x_0}^{p^k+1}). \end{aligned}$$

Hence $n(\alpha, \beta, a)$ is well-defined (independent of the choice of x_0).

If (i) is satisfied, that is, $\phi_{\alpha,\beta}(x) + \gamma = 0$ has solution(s) in $\mathbb{F}_q$ which yields that $2XH_{\alpha,\beta} + A_\gamma = 0$ has solution(s). Note that $\operatorname{rank} H_{\alpha,\beta} = s - i$. Therefore $2XH_{\alpha,\beta} + A_\gamma = 0$ has $q_0^i = p^{id}$ solutions with $X \in \mathbb{F}_{q_0}^s$ which is equivalent to saying $\phi_{\alpha,\beta}(x) + \gamma = 0$ has p^{id} solutions in $\mathbb{F}_q$. Conversely, for any $x_0 \in \mathbb{F}_q$, we

can determine γ by $\gamma = -\phi_{\alpha,\beta}(x_0)$. Let $N(\alpha,\beta,a)$ be the number of $x_0 \in \mathbb{F}_q$ satisfying (ii). Then we have $n(\alpha,\beta,a) = N(\alpha,\beta,a)/p^{id}$.

Let $\chi'(x) = \zeta_p^{\mathrm{Tr}_1^t(x)}$ with $x \in \mathbb{F}_{p^t}$ be an additive character on $\mathbb{F}_{p^t}$ and $G(\eta',\chi') = \sum_{x\in\mathbb{F}_{p^t}} \eta'(x)\chi'(x)$ be the Gaussian sum on $\mathbb{F}_{p^t}$. We can calculate

$$\begin{aligned} p^t \cdot N(\alpha,\beta,a) &= \sum_{x\in\mathbb{F}_q}\sum_{\omega\in\mathbb{F}_{p^t}} \zeta_p^{\mathrm{Tr}_1^t\left(\omega\cdot\left(\mathrm{Tr}_t^m(\alpha x^{p^m+1})+\mathrm{Tr}_t^n(\beta x^{p^k+1})-a\right)\right)} \\ &= p^n + \sum_{\omega\in\mathbb{F}_{p^t}^*} T(\omega\alpha,\omega\beta)\zeta_p^{-\mathrm{Tr}_1^t(a\omega)} \\ &= p^n + T(\alpha,\beta)\cdot \sum_{\omega\in\mathbb{F}_{p^t}^*} \eta_0(\omega)^{s-i}\chi'(-a\omega) \end{aligned}$$

where the 3-rd equality holds from (19) for any $\omega \in \mathbb{F}_{p^t}^* \subset \mathbb{F}_{q_0}^*$.

- If $s-i$ and d/t are both odd, and $a=0$, then $\eta_0(\omega)^{s-i} = \eta'(\omega)$ and $N(\alpha,\beta,0) = p^{n-t}$.
- If $s-i$ and d/t are both odd, and $a \neq 0$, then

$$\begin{aligned} N(\alpha,\beta,a) &= p^{n-t} + \tfrac{1}{p^t}\cdot T(\alpha,\beta)\cdot \sum_{\omega\in\mathbb{F}_{p^t}^*} \eta_0(\omega)\chi'(-a\omega) \\ &= p^{n-t} + \tfrac{1}{p^t}\cdot T(\alpha,\beta)\cdot\eta'(-a)\cdot G(\eta',\chi') \\ &= p^{n-t} + \varepsilon\eta'(a)p^{\frac{n+id-t}{2}} \end{aligned}$$

  where the 2-nd equality follows from the explicit evaluation of quadratic Gaussian sums (see [13], Theorem 5.15 and 5.33).

- If $s-i$ or d/t is even, and $a=0$, then $\eta_0(\omega)^{s-i} = 1$ for any $\omega \in \mathbb{F}_{p^t}^*$ and $N(\alpha,\beta,0) = p^{n-t} + \varepsilon(p^t-1)p^{\frac{n+id}{2}-t}$.
- If $s-i$ or d/t is even, and $a \neq 0$, then

$$\begin{aligned} N(\alpha,\beta,a) &= p^{n-t} + \tfrac{1}{p^t}\cdot T(\alpha,\beta)\cdot \sum_{\omega\in\mathbb{F}_{p^t}^*} \chi'(-a\omega) \\ &= p^{n-t} - \varepsilon p^{\frac{n+id}{2}-t}. \end{aligned}$$

Therefore we complete the proof by dividing p^{id}. □

Proof of Theorem 3: Define

$$\Xi = \left\{(\alpha,\beta,\gamma)\in\mathbb{F}_q^3 \,|S(\alpha,\beta,\gamma)=0\right\}$$

and $\xi = \left|\Xi\right|$.

Recall $n_i, H_{\alpha,\beta},, r_{\alpha,\beta}, A_\gamma$ in Section 1 and $N_{i,\varepsilon}, n_{i,\varepsilon,}$ in the proof of Lemma 2. Note that $2XH_{0,0}+A_\gamma=0$ is solvable if and only if $\gamma=0$. If $(\alpha,\beta)\in N_{i,\varepsilon}$, then the number of $\gamma\in\mathbb{F}_q$ such that $2XH_{\alpha,\beta}+A_\gamma=0$ is solvable is $q_0^{s-i}=p^{n-id}$. From Lemma 2 (i) we know that

- if $d'=d$ and $(\alpha,\beta)\neq(0,0)$, then $r_{\alpha,\beta}=s-i$ for some $i\in\{0,1,2\}$. By Lemma 1 (ii) we have

$$\begin{aligned}\xi &= p^n-1+(p^n-p^{n-d})n_1+(p^n-p^{n-2d})n_2\\ &= (p^n-1)(p^{3m-d}-p^{3m-2d}+p^{3m-3d}-p^{n-2d}+1).\end{aligned} \tag{32}$$

- if $d'=2d$, similarly we have

$$\begin{aligned}\xi &= p^n-1+(p^n-p^{n-2d})n_{2,1}+(p^n-p^{n-4d})n_{4,-1}\\ &= (p^n-1)(p^{3m-d}-p^{3m-2d}+p^{3m-3d}-p^{3m-4d}+p^{3m-5d}\\ &\qquad +p^{n-d}-2p^{n-2d}+p^{n-3d}-p^{n-4d}+1).\end{aligned} \tag{33}$$

Assume $(\alpha,\beta)\in N_{i,\varepsilon}$ and $\phi_{\alpha,\beta}(x)+\gamma=0$ has solution(s) in $\mathbb{F}_q$ (choose one, say x_0). Then by Lemma 1 we get

$$S(\alpha,\beta,\gamma)=\zeta_p^{-\left(\mathrm{Tr}_t^m(\alpha x_0^{p^m+1})+\mathrm{Tr}_t^n(\beta x_0^{p^k+1})\right)}\cdot T(\alpha,\beta).$$

Applying Lemma 6 for $t=1$ and Theorem 1, we get the result. $\square$

Proof of Theorem 4: Recall $M_{(\alpha_1,\beta_1),(\alpha_2,\beta_2)}(\tau)$ defined in (6) and (7). Fix $(\alpha_2,\beta_2)\in\mathbb{F}_{p^m}\times\mathbb{F}_q$, when (α_1,β_1) runs through $\mathbb{F}_{p^m}\times\mathbb{F}_q$ and τ takes value from 0 to $q-2$, (α',β',γ') runs through $\mathbb{F}_{p^m}\times\mathbb{F}_q\times\left\{\mathbb{F}_q\backslash\{1\}\right\}$ exactly one time.

For any possible value κ of $S(\alpha,\beta,\gamma)$, define

$$s_\kappa = \#\left\{(\alpha,\beta,\gamma)\in\mathbb{F}_{p^m}\times\mathbb{F}_q\times\mathbb{F}_q \,|\, S(\alpha,\beta,\gamma)=\kappa\right\}$$

$$s_\kappa^1 = \#\left\{(\alpha,\beta,\gamma)\in\mathbb{F}_{p^m}\times\mathbb{F}_q\times\{\mathbb{F}_q\backslash\{1\}\}\;\middle|\; S(\alpha,\beta,\gamma)=\kappa\right\}$$

and

$$t_\kappa = \#\left\{(\alpha,\beta)\in\mathbb{F}_{p^m}\times\mathbb{F}_q \,|\, T(\alpha,\beta)=\kappa\right\}.$$

By Lemma 7 we have

$$s_\kappa^1 = \frac{q-2}{q-1}\times(s_\kappa - t_\kappa) + t_\kappa = \frac{q-2}{q-1}\times s_\kappa + \frac{1}{q-1}\times t_\kappa.$$

Define M_κ to be the number of $(\alpha_1,\beta_1,\alpha_2,\beta_2)$ such that $M_{(\alpha_1,\beta_1),(\alpha_2,\beta_2)}=\kappa$. Hence we get

$$M_\kappa = p^{3m}\cdot s_\kappa^1 = p^{3m}\cdot\left(\frac{q-2}{q-1}\cdot s_\kappa + \frac{1}{q-1}\cdot t_\kappa\right).$$

Then the result follows from Theorem 1 and Theorem 3. □

Proof of Theorem 5: From (1) we know that for each non-zero codeword $c(\alpha,\beta,\gamma)=(c_0,\cdots,c_{q-2})$ ($c_i=\mathrm{Tr}_t^m(\alpha\pi^{(p^m+1)i})+\mathrm{Tr}_t^n(\beta\pi^{(p^k+1)i}+\gamma\pi^i)$, $0\le i\le q-2$, and $(\alpha,\beta,\gamma)\in\mathbb{F}_{p^m}\times\mathbb{F}_q^2$), the Hamming weight of $c(\alpha,\beta,\gamma)$ is

$$w_H\left(c(\alpha,\beta,\gamma)\right) = p^{n-t}(p^t-1) - \frac{1}{p^t}\cdot R(\alpha,\beta,\gamma) \tag{34}$$

where

$$R(\alpha,\beta,\gamma) = \sum_{\omega\in\mathbb{F}_{p^t}^*} S(\omega\alpha,\omega\beta,\omega\gamma).$$

For any $\omega\in\mathbb{F}_{p^t}^*\subset\mathbb{F}_{q_0}^*$, we have $\phi_{\omega\alpha,a\beta}(x)+\omega\gamma=0$ is equivalent to $\phi_{\alpha,\beta}(x)+\gamma=0$. Let $x_0\in\mathbb{F}_q$ be a solution of $\phi_{\alpha,\beta}(x)+\gamma=0$ (if exist).

(1). If $\phi_{\alpha,\beta}(x)+\gamma=0$ has solutions in $\mathbb{F}_q$, then by Lemma 1 and (19) we have

$$\begin{aligned}S(\omega\alpha,\omega\beta,\omega\gamma) &= \zeta_p^{-\left(\mathrm{Tr}_1^m(\omega\alpha x_0^{p^m+1})+\mathrm{Tr}_1^n(\omega\beta x_0^{p^k+1})\right)} T(\omega\alpha,\omega\beta)\\ &= \zeta_p^{-\left(\mathrm{Tr}_1^m(\omega\alpha x_0^{p^m+1})+\mathrm{Tr}_1^n(\omega\beta x_0^{p^k+1})\right)} \eta_0(\omega)^{r_{\alpha,\beta}} T(\alpha,\beta).\end{aligned}$$

Hence

$$R(\alpha,\beta,\gamma) = T(\alpha,\beta)\sum_{\omega\in\mathbb{F}_{p^t}^*}\zeta_p^{-\mathrm{Tr}_1^t\left(\omega\cdot\left(\mathrm{Tr}_t^m(\alpha x_0^{p^m+1})+\mathrm{Tr}_t^n(\beta x_0^{p^k+1})\right)\right)}\eta_0(\omega)^{r_{\alpha,\beta}}.$$

Fix $(\alpha,\beta)\in N_{i,\varepsilon}$ for $\varepsilon=\pm1$, and suppose $\phi_{\alpha,\beta}(x)+\gamma=0$ is solvable in $\mathbb{F}_q$. Denote by $\vartheta=\mathrm{Tr}_t^m(\alpha x_0^{p^m+1})+\mathrm{Tr}_t^n(\beta x_0^{p^k+1})$. Then

– if $s-i$ and d/t are both odd, and $\vartheta = 0$, then

$$R(\alpha,\beta,\gamma) = T(\alpha,\beta)\sum_{\omega\in\mathbb{F}_{p^t}^*}\eta'(\omega) = 0.$$

– if $s-i$ and d/t are both odd, and $\vartheta \neq 0$, then by the result of quadratic Gaussian sums

$$\begin{array}{rcl} R(\alpha,\beta,\gamma) & = & T(\alpha,\beta)\eta'(-\vartheta)G(\eta',\chi') \\ & = & \varepsilon\eta'(\vartheta)p^{\frac{n+id+t}{2}}, \\ & = & \begin{cases} p^{m+\frac{id+t}{2}} & \text{if } \varepsilon = \eta'(\vartheta), \\ -p^{m+\frac{id+t}{2}} & \text{if } \varepsilon = -\eta'(\vartheta). \end{cases} \end{array}$$

– if $s-i$ or d/t is even, and $\vartheta = 0$, then $\eta_0(\omega)^{r_{\alpha,\beta}} = 1$ for $\omega \in \mathbb{F}_{p^t}^*$ and $R(\alpha,\beta,\gamma) = (p^t-1)T(\alpha,\beta) = \varepsilon(p^t-1)p^{m+\frac{id}{2}}$.

– if $s-i$ or d/t is even, and $\vartheta \neq 0$, then $\eta_0(\omega)^{r_{\alpha,\beta}} = 1$ for $\omega \in \mathbb{F}_{p^t}^*$ and $R(\alpha,\beta,\gamma) = -T(\alpha,\beta) = -\varepsilon p^{m+\frac{id}{2}}$.

(2). If $\phi_{\alpha,\beta}(x)+\gamma = 0$ has no solutions in $\mathbb{F}_q$ which implies that $\phi_{\omega\alpha,\omega\beta}(x)+\omega\gamma = 0$ also has no solutions in $\mathbb{F}_q$ for any $\omega \in \mathbb{F}_{p^t}^* \subset \mathbb{F}_{q_0}$. Hence $S(\omega\alpha,\omega\beta,\omega\gamma) = 0$ and $R(\alpha,\beta,\gamma) = 0$.

Thus the weight distribution of $\mathcal{C}_2$ can be derived from Theorem 1, Lemma 6, (32), (33) and (34) directly. □

8 Conclusion

In this paper we have studied the exponential sums $\sum_{x\in\mathbb{F}_q}\zeta_p^{\mathrm{Tr}_1^m(\alpha x^{p^m+1})+\mathrm{Tr}_1^n(\beta x^{p^k+1})}$ and $\sum_{x\in\mathbb{F}_q}\zeta_p^{\mathrm{Tr}_1^m(\alpha x^{p^m+1})+\mathrm{Tr}_1^n(\beta x^{p^k+1}+\gamma x)}$ with $\alpha \in \mathbb{F}_{p^m}, (\beta,\gamma) \in \mathbb{F}_q^2$. After giving the value distribution of $\sum_{x\in\mathbb{F}_q}\zeta_p^{\mathrm{Tr}_1^m(\alpha x^{p^m+1})+\mathrm{Tr}_1^n(\beta x^{p^k+1})}$ and $\sum_{x\in\mathbb{F}_q}\zeta_p^{\mathrm{Tr}_1^m(\alpha x^{p^m+1})+\mathrm{Tr}_1^n(\beta x^{p^k+1}+\gamma x)}$, we determine the correlation distribution among a family of sequences, and the weight distributions of the cyclic codes $\mathcal{C}_1$ and $\mathcal{C}_2$. These results generalize [30].

9 Acknowledgements

The authors will thank the anonymous referees for their helpful comments.

References

[1] A.W. Bluher, "On $x^{q+1} + ax + b$," *Finite Fields and Their Appli.,* vol. 10, pp. 285–305, 2004.

[2] R.S. Coulter, "Explicit evaluation of some Weil sums," *Acta Arith.,* vol. 83, no. 3, pp. 241–251, 1998.

[3] K. Feng and J. Luo, "Value distribution of exponential sums from perfect nonlinear functions and their applications," *IEEE Trans. Inf. Theory,* vol. 53, no. 9, pp. 3035–3041, Sept. 2007.

[4] K. Feng and J. Luo, "Weight distribution of some reducible cyclic codes," *Finite Fields and Their Appli.*, vol. 14, no. 4, pp. 390–409, April 2008.

[5] R.W. Fitzgerald, J.L. Yucas, "Sums of Gauss sums and weights of irreducible codes," *Finite Fields and Their Appli.,* vol. 11, pp. 89–110, 2005.

[6] R. Gold, "Maximal recursive sequences with 3-valued recursive cross-correlation functions," *IEEE Trans. Inf. Theory,* vol. 14, no. 1, pp. 154–156, Jan. 1968.

[7] T. Helleseth and P.V. Kumar, "Sequences with low correlation," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: North-Holland, 1998.

[8] T. Helleseth, J. Lahtonen and P. Rosendahl, "On Niho type cross-correlation functions of m-sequences", *Finite Fields and Their Appli.,* vol. 13, no. 2, pp. 305–317, April 2007.

[9] J. Luo and K. Feng, "On the weight distribution of two classes of cyclic codes," *IEEE Trans. Inf. Theory,* vol. 54, no. 12, pp. 5332–5344, Dec. 2008.

[10] J. Luo and K. Feng, "Cyclic codes and sequences from generalized Coulter-Matthews function," *IEEE Trans. Inf. Theory,* vol. 54, no. 12, pp. 5345–5353, Dec. 2008.

[11] T. Kasami, “Weight distribution of Bose-Chaudhuri-Hocquenghem codes,” in Combinatorial Mathematics and Its Applications. R. C. Bose and T. A. Dowling, Eds. Chapel Hill, NC: Univerisity of North Carolina Press, 1969, pp. 335–357.

[12] T. Kasami, “Weight distribution formula for some class of cyclic codes,” Coordinated Sci. Lab., Univ. Illinois, Urabana-Champaign, Tech. Rep. R-285(AD 635274), 1966.

[13] R. Lidl, and H. Niederreiter, Finite Fields, Addison-Wesley, Encyclopedia of Mathematics and its Applications, vol. 20, 1983.

[14] R.J. McEliece, “Irreducible cyclic codes and Gauss sums,” in : *Combinatorics, Part I: Theory of Designs, Finite Geometry and Coding Theory,* Math Centre Tracts, Amsterdam: Math. Centrum, no. 55, pp. 179–196, 1974.

[15] J. Lahtonen, “Two remarks on a paper by Moreno and Kumar,” *IEEE Trans. Inf. Theory,* vol. 41, no. 3, pp. 859–861, May 1995.

[16] R.J. McEliece and H. Rumsey Jr., “Euler products, cyclotomy, and coding,” *J. Number Theory,* vol. 4, pp. 302–311, 1972.

[17] O. Moreno and P.V. Kumar, “Minimum distance bounds for cyclic codes and Deligne’s Theorem,” *IEEE Trans. Inf. Theory,* vol. 39, no. 5, pp. 1524–1534, Sept. 1993.

[18] G. Ness, T. Helleseth, and A. Kholosha, “On the correlation distribution of the Coulter-Matthews decimation,” *IEEE Trans. Inf. Theory,* vol. 52, no. 5, pp. 2241–2247, May 2006.

[20] P. Rosendahl, “A generalization of Niho’s theorem,” *Des.Codes Crypto.,* vol. 38, no. 3, pp.331–336, March 2006.

[21] P. Rosendahl, “Niho type cross-correlation functions and related equations,” Ph.D dissertation, Depart. Math., Univ. Turku, Finland, 2004.

[22] R. Schoof, “Families of curves and weight distribution of codes,” *Bull. of Amer. Math. Society,* vol. 32, no. 2, pp. 171–183, 1995.

[23] H.M. Trachtenberg, “On the cross-correlation function of maximal linear sequences,” Ph.D dissertation, Univ. South. Calif. Los Angles, 1970.

[24] M. Van Der Vlugt, "Hasse-Davenport curve, Gauss sums and weight distribution of irreducible cyclic codes," *J. of Number Theory* vol. 55, pp. 145–159, 1995.

[25] M. Van Der Vlugt, "Surfaces and the weight distribution of a family of codes," *IEEE Trans. Inf. Theory,* vol. 43, no. 4, pp. 1354–1360, Apri. 1997.

[26] J. Wolfmann, "Weight distribution of some binary primitive cylcic codes," *IEEE Trans. Inf. Theory,* vol. 40, no. 6, pp. 2068–2071, Jun. 2004.

[27] Y. Xia, X. Zeng, and L. Hu, "The large set of p-ary Kasami sequences", preprint.

[28] J. Yuan, C. Carlet and C. Ding, "The weight distribution of a class of linear codes from perfect nonlinear functions," *IEEE Trans. Inf. Theory,* vol. 52, no. 2, pp. 712–717, Feb. 2006.

[29] X. Zeng, J.Q. Liu and L. Hu, "Generalized Kasami sequences: the large set," *IEEE Trans. Inf. Theory,* vol. 53, no. 7, pp. 2578–2598, July 2007.

[30] X. Zeng, N. Li and L. Hu, "A class of nonbinary codes and their weight distribution," see http://arxiv.org/abs/0802.3430, preprint.